Kvantové počítání

Pavel Cejnar

ÚČJF MFF UK Praha
pavel.cejnar@mff.cuni.cz

Program:
1) Historie
2) Principy
3) Příklady
4) Realizace

Nové Strašecí, leden 2016

Kvantové počítání

1) **Historie**
2) Principy
3) Příklady
4) Realizace

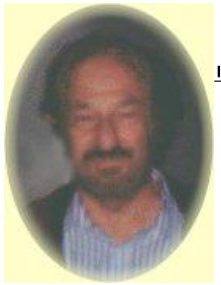
Rolf Landauer (1927-1999)

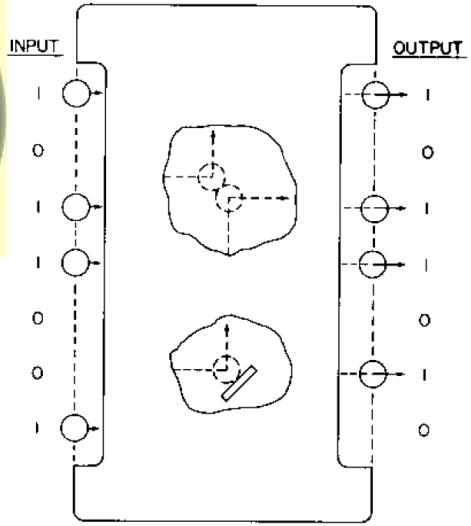
Prehistorie

1960-70s: Analýzy fyzikálních omezení klasických počítačů
„Vratné počítače“ (počítání založené na reverzibilních procesech)

1959: Feynman pronesl řeč „*There's Plenty of Room at the Bottom*”
1960: První úvahy o fyzikálních mezích miniaturizace výpočetních procesů
1961: Landauer ukázal, že každý ireverzibilní krok výpočtu produkuje entropii-teplo
1969: První návrh „spinového počítače“ (kvantové vlastnosti chápány spíš jako omezení)
1973: Benett předkládá koncept univerzálního reverzibilního počítače
1981: Fredkin & Toffoli demonstrují výpočetní reverzibilitu na “*billiard ball computer*”

Edward Fredkin

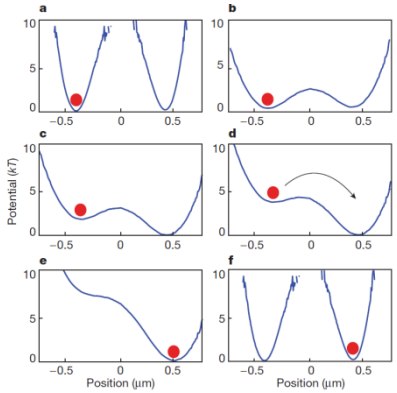


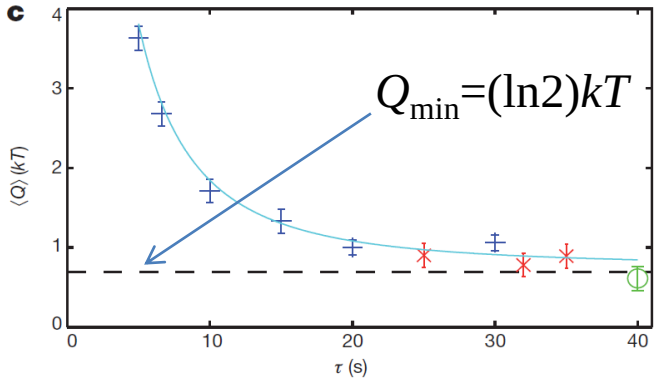


LETTER 8 MARCH 2012 | VOL 483 | NATURE | 187
doi:10.1038/nature10872

Experimental verification of Landauer's principle linking information and thermodynamics

Antoine Bérut[1], Artak Arakelyan[1], Artyom Petrosyan[1], Sergio Ciliberto[1], Raoul Dillenschneider[2] & Eric Lutz[3]†





Richard Phillips Feynman (1918-1988)

Počátek

1960-70s: Analýzy fyzikálních omezení klasických počítačů

1980-81: První úvahy o prospěšnosti QM pro teorii počítání

Richard Feynman, Jurij Manin, ...

4. QUANTUM COMPUTERS—UNIVERSAL QUANTUM SIMULATORS

program that Fredkin is always pushing, about trying to find a computer simulation of physics, seem to me to be an excellent program to follow out. He and I have had wonderful, intense, and interminable arguments, and my argument is always that the real use of it would be with quantum mechanics, and therefore full attention and acceptance of the quantum mechanical phenomena—the challenge of explaining quantum mechanical phenomena—has to be put into the argument, and therefore these phenomena have to be understood very well in analyzing the situation. And I'm not happy with all the analyses that go with just the classical theory, because nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy. Thank you.

International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain.

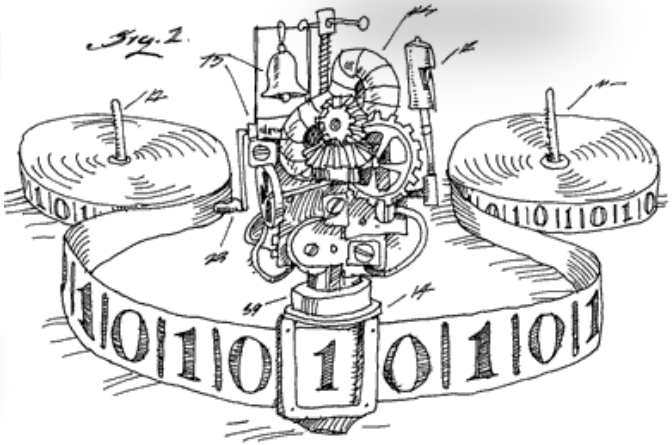
Richard Phillips Feynman (1918-1988)

Expanze

1960-70s: Analýzy fyzikálních omezení klasických počítačů

1980-81: První úvahy o prospěšnosti QM pro teorii počítání
Richard Feynman, Jurij Manin, ...

1985: Kvantový Turingův stroj
1989: Elementární kvantové operace
David Deutsch



1994: Kvantový faktorizační algoritmus
Peter Shor

$$N = P_1 \cdot P_2 \begin{cases} P_1, P_2 \Rightarrow N \checkmark \\ N \Rightarrow P_1, P_2 \text{ X} \end{cases}$$

RSA šifrování: Nejprve si bude Alice muset vyrobit pár veřejného a soukromého klíče: Zvolí dvě různá velká náhodná prvočísla p a q. Spočítá jejich součin n = pq. Spočítá hodnotu Eulerovy funkce ϕ(n) = (p − 1)(q − 1). Zvolí celé číslo e menší než ϕ(n), které je s ϕ(n) nesoudělné. Nalezne číslo d tak, aby platilo de ≡ 1 (mod ϕ(n)), kde symbol ≡ značí kongruenci zbytkových tříd. Jestli e je prvočíslo, tak d = (1+r*ϕ(n))/e, kde r = [(e-1)ϕ(n)^(e-2)]. Veřejným klíčem je dvojice (n, e), přičemž n se označuje jako modul, e jako šifrovací či veřejný exponent. Soukromým klíčem je dvojice (n, d), kde d se označuje jako dešifrovací či soukromý exponent. V praxi se klíče uchovávají v mírně upravené formě, která umožňuje rychlejší zpracování. Veřejný klíč poté Alice uveřejní, respektive zcela otevřeně pošle Bobovi. Soukromý klíč naopak uchová v tajnosti. (Wikipedie)

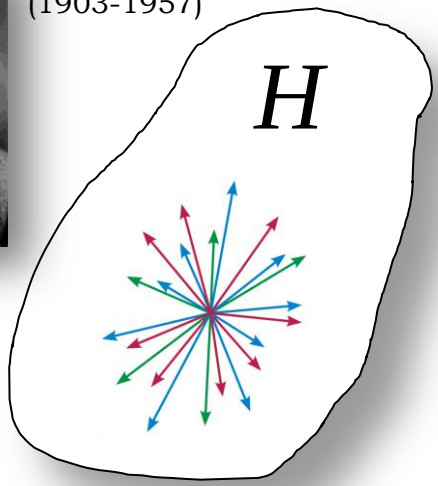
Kvantové počítání

1) Historie
2) **Principy**
3) Příklady
4) Realizace

Tři zdroje
kvantového počítání

Erwin Schrödinger (1887–1961)

John von Neumann (1903-1957)



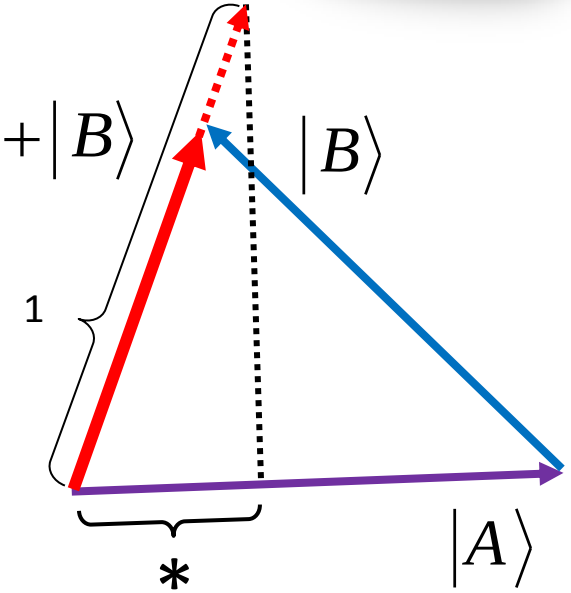
1) Kvantová neurčitost

Stavy kvantových systémů reprezentovány vektory

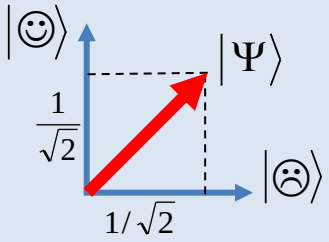
„superpozice“ $|\Psi\rangle = \alpha|A\rangle + \beta|B\rangle$

Vektory mají nenulový „překryv“ **=>** stavy nejsou dokonale rozlišitelné

$$|*|^2 = \begin{cases} \text{pravděpodobnost} \\ \text{vzájemné záměny} \\ \text{obou stavů} \end{cases}$$



$$|\Psi\rangle = \frac{1}{\sqrt{2}}|\text{☺}\rangle + \frac{1}{\sqrt{2}}|\text{☹}\rangle$$

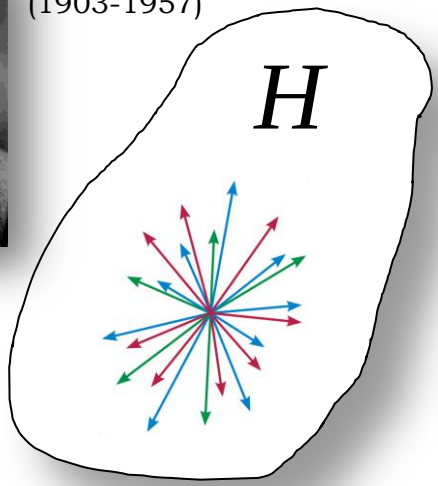


$$P(\text{☺}) = \frac{1}{2} = P(\text{☹})$$

Tři zdroje
kvantového počítání

Erwin Schrödinger (1887–1961)

John von Neumann (1903-1957)

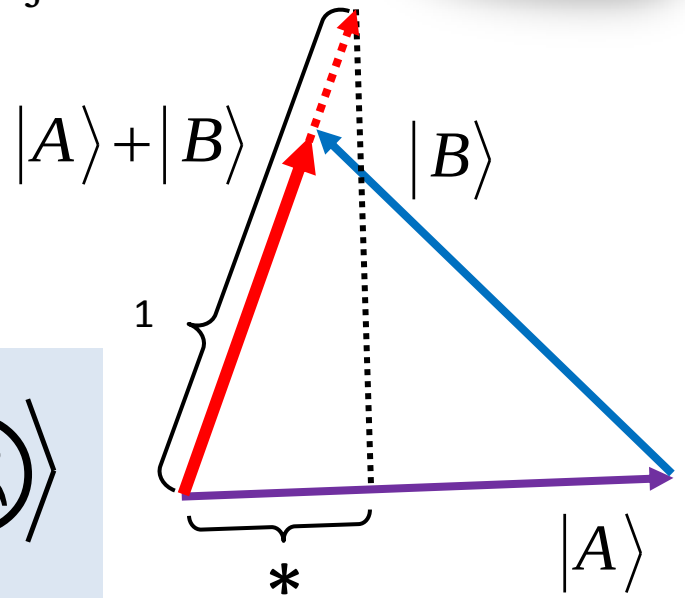


1) Kvantová neurčitost

Stavy kvantových systémů reprezentovány vektory

„**superpozice**“ $|\Psi\rangle = \alpha|A\rangle + \beta|B\rangle$

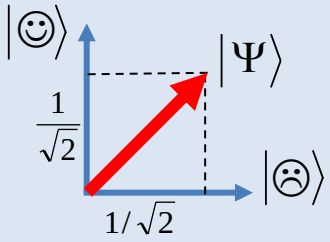
Vektory mají nenulový „překryv“ **=>** stavy nejsou dokonale rozlišitelné



2) Vlastnosti kvantových měření

Výsledky měření mají **pravděpodobnostní charakter**. Měření **mění stav systému**

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|☺\rangle + \frac{1}{\sqrt{2}}|☹\rangle$$

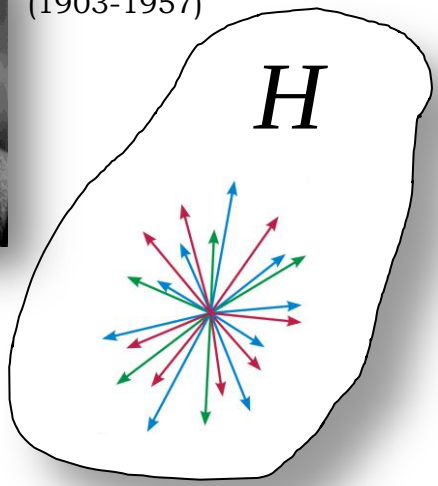


$$P(☺) = \frac{1}{2} = P(☹)$$

Tři zdroje
kvantového počítání

Erwin Schrödinger (1887–1961)

John von Neumann (1903-1957)



1) Kvantová neurčitost

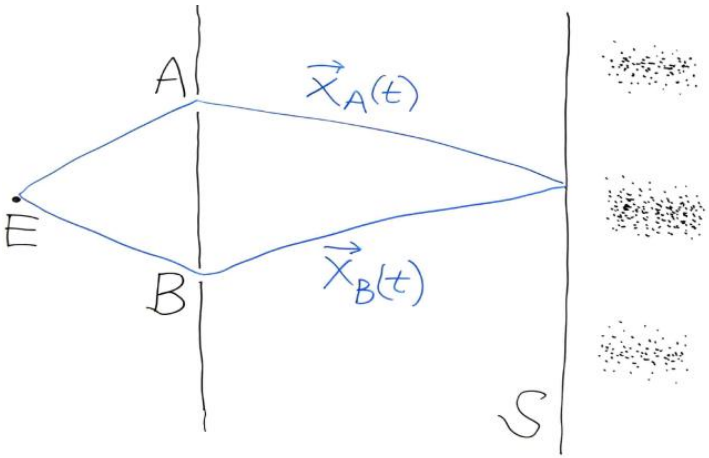
Stavy kvantových systémů reprezentovány vektory

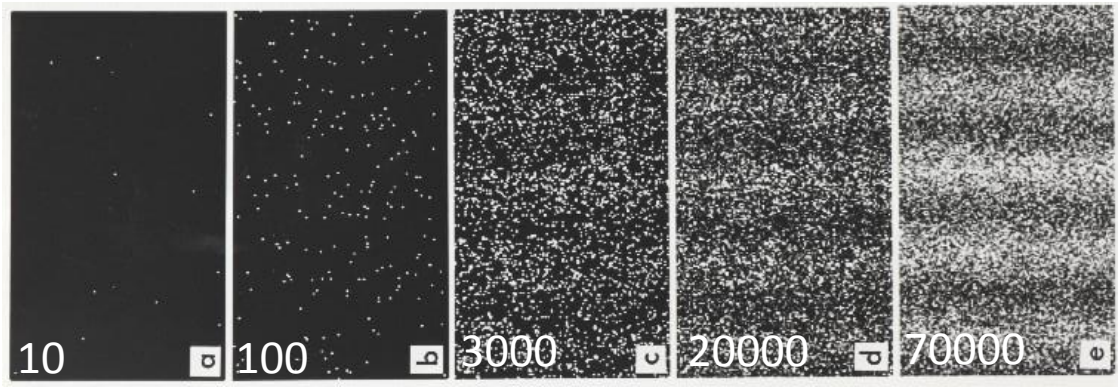
„**superpozice**“ $|\Psi\rangle = \alpha|A\rangle + \beta|B\rangle$

Vektory mají nenulový „překryv“ **=>** stavy nejsou dokonale rozlišitelné

2) Vlastnosti kvantových měření

Výsledky měření mají **pravděpodobnostní charakter**. Měření **mění stav systému**

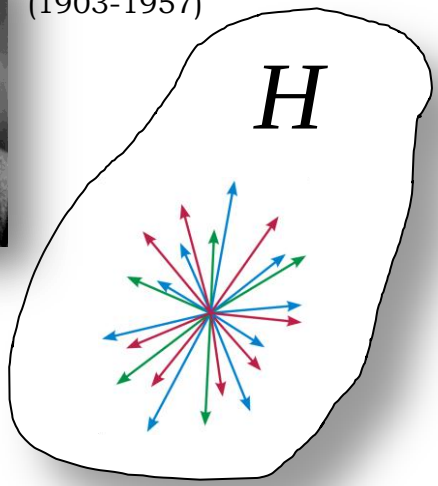




Tři zdroje
kvantového počítání

Erwin Schrödinger (1887–1961)

John von Neumann (1903-1957)



1) Kvantová neurčitost

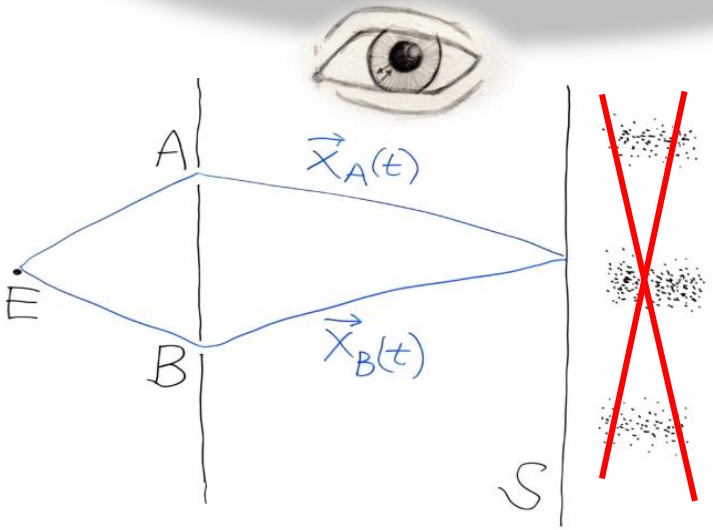
Stavy kvantových systémů reprezentovány vektory

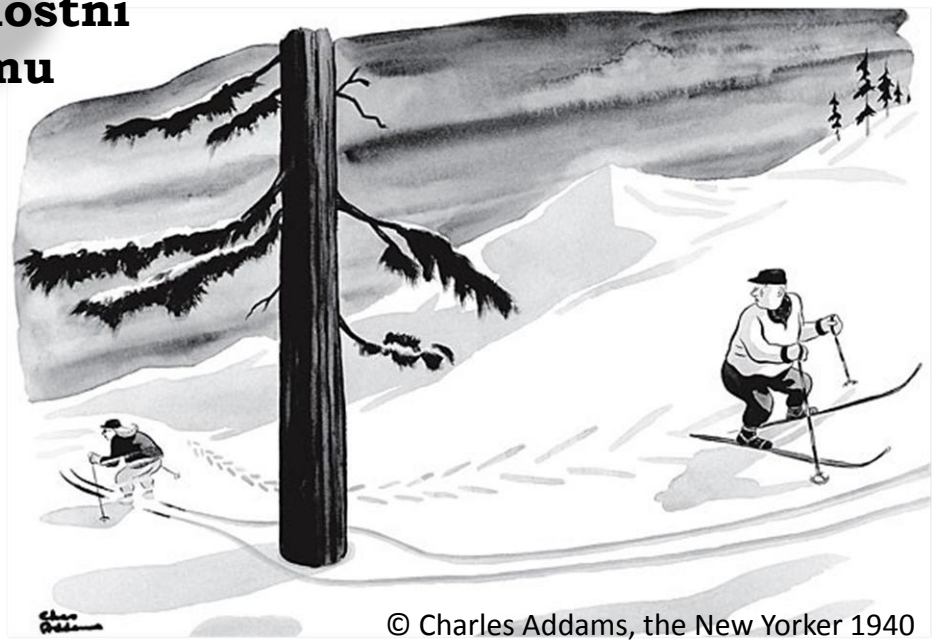
„**superpozice**“ $|\Psi\rangle = \alpha|A\rangle + \beta|B\rangle$

Vektory mají nenulový „překryv“ **=>** stavy nejsou dokonale rozlišitelné

2) Vlastnosti kvantových měření

Výsledky měření mají **pravděpodobnostní charakter**. Měření **mění stav systému**

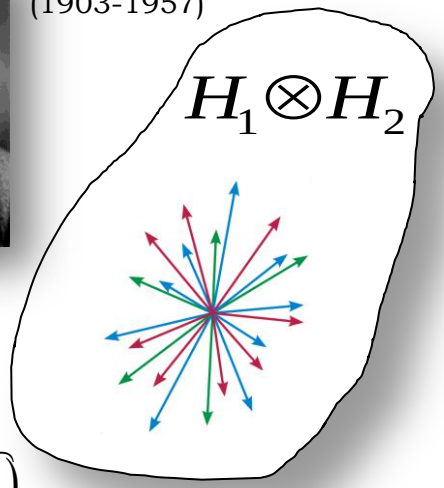




Tři zdroje
kvantového počítání

Erwin Schrödinger
(1887–1961)

John von Neumann
(1903-1957)



3) Kvantová provázanost

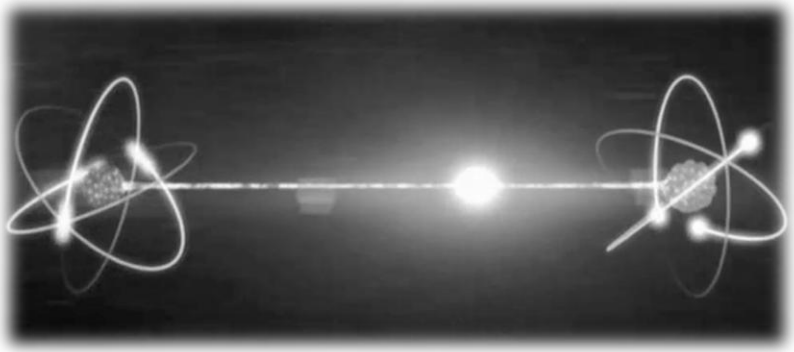
Stavy složených systémů jsou reprezentovány vektory v součinovém prostoru

Např. $|\Psi\rangle = \alpha|A_1\rangle|B_2\rangle + \beta|B_1\rangle|A_2\rangle \neq \overbrace{(\alpha_1|A_1\rangle + \beta_1|B_1\rangle)}^{|\Psi_1\rangle}\overbrace{(\alpha_2|A_2\rangle + \beta_2|B_2\rangle)}^{|\Psi_2\rangle}$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|\text{☹}\rangle|\text{☺}\rangle + \frac{1}{\sqrt{2}}|\text{☺}\rangle|\text{☹}\rangle$$

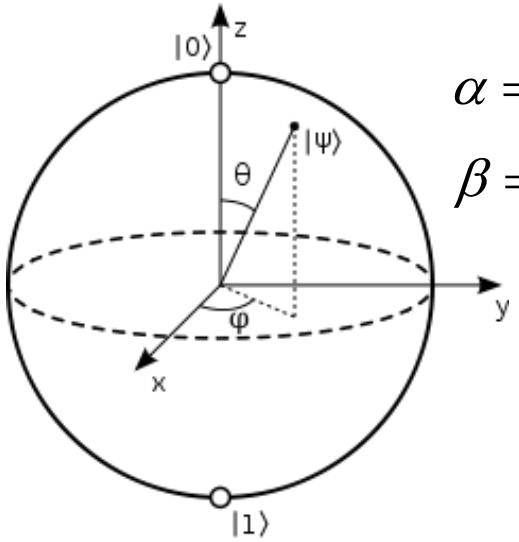
Cejnar Doležal Cejnar Doležal

Provázaný stav => podsystémy nemají své vlastní stavové vektory, nedají se popsat odděleně, nýbrž vykazují (bez ohledu na vzdálenost) silné **kvantové korelace**



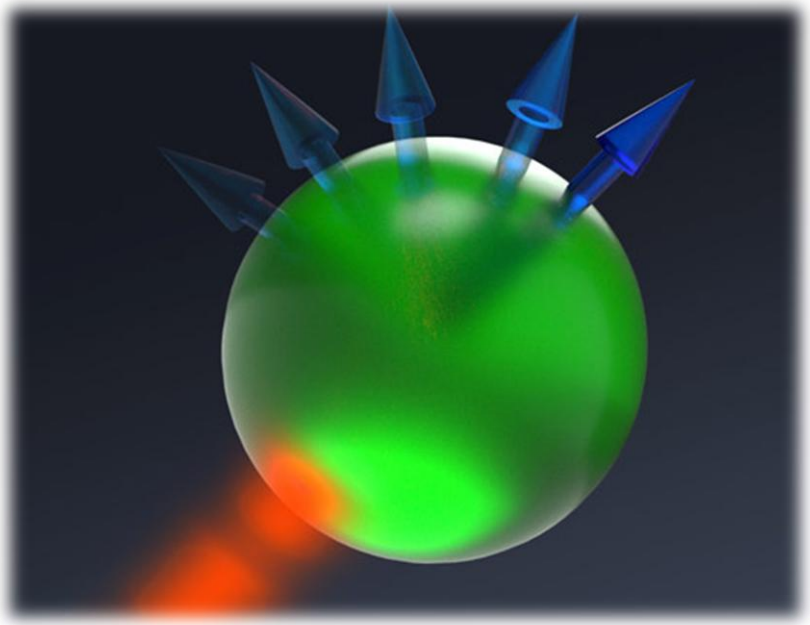
Kvantový bit = **qubit**, Qbit, qbit, „*kvabit*“ …

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



$$\alpha = \cos\frac{\theta}{2}$$

$$\beta = e^{i\phi}\sin\frac{\theta}{2}$$



Možné fyzikální realizace

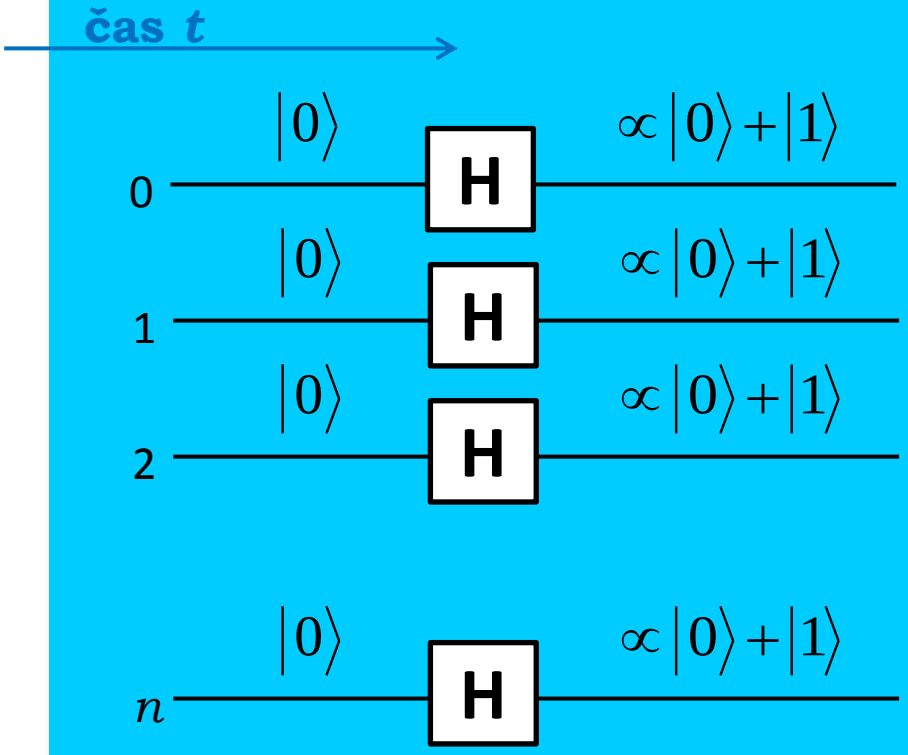
- Projekce spinu elektronu, protonu, lichého jádra…(s=½)
- Lineární/kruhové polarizační stavy fotonu
- Dva vybrané energetické stavy atomu
- Proudové stavy supravodivého prstence….

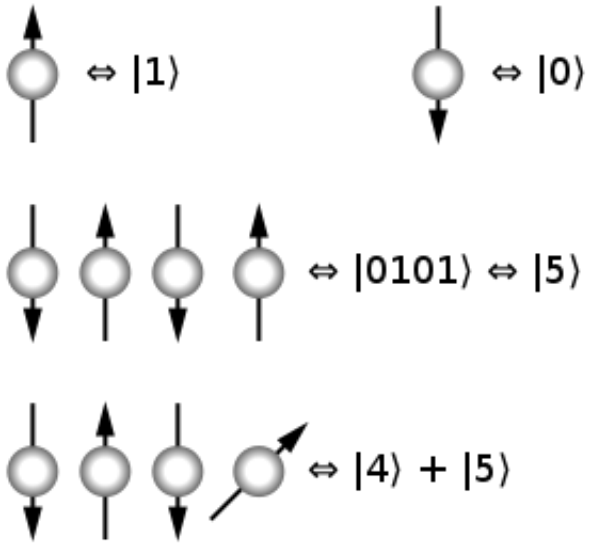
Kvantový registr

Obecný stav *n*-tice qbitů = superpozice všech číselných hodnot

$$|\Psi\rangle = \alpha_0 \underbrace{|0\cdots00\rangle}_{|0\rangle} + \alpha_1 \underbrace{|0\cdots01\rangle}_{|1\rangle} + \alpha_2 \underbrace{|0\cdots10\rangle}_{|2\rangle} + \cdots + \alpha_{2^n-1} \underbrace{|11\cdots1\rangle}_{|2^n-1\rangle}$$

Příprava homogenní superpozice:





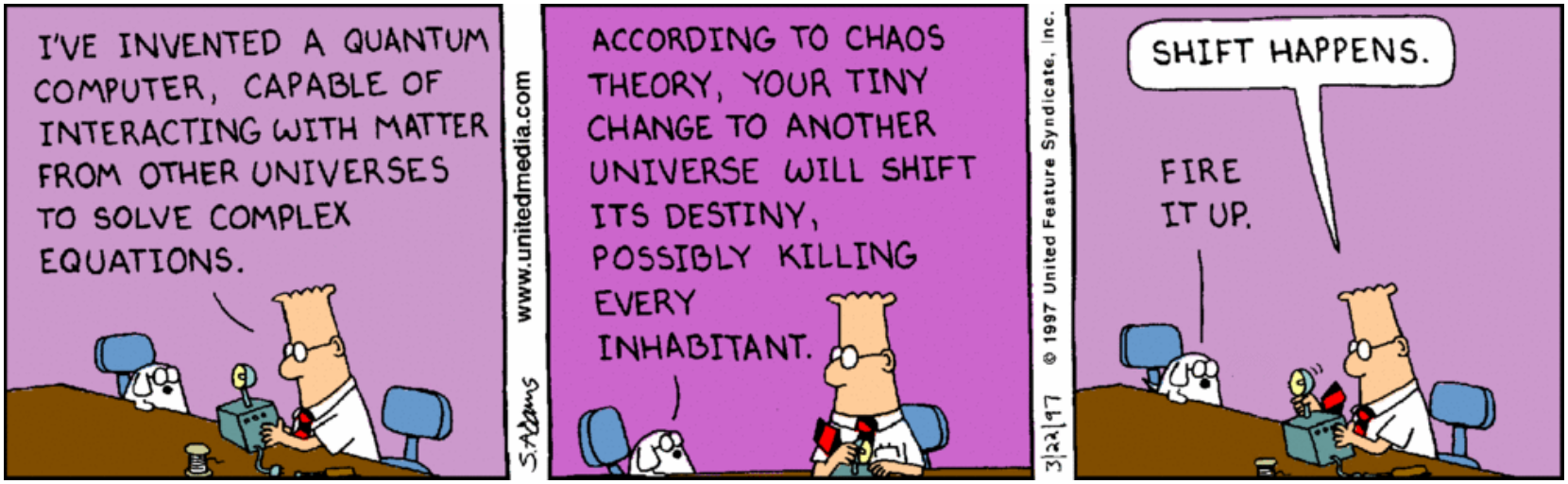
Kvantový výpočet

Krokovaná kvantová **evoluce** stavu počítače a následné **měření**

$$\underbrace{\hat{U}_N \hat{U}_{N-1} \cdots \hat{U}_2 \hat{U}_1}_{\hat{U}(N)} \left|\Psi(0)\right\rangle \equiv \left|\Psi(N)\right\rangle = \alpha_0(N)\left|0\right\rangle + \alpha_1(N)\left|1\right\rangle + \cdots \alpha_{2^n-1}(N)\left|2^{n-1}\right\rangle$$

….**opakování** výpočtu a statistické vyhodnocení výstupů

Co na to Dilbert?

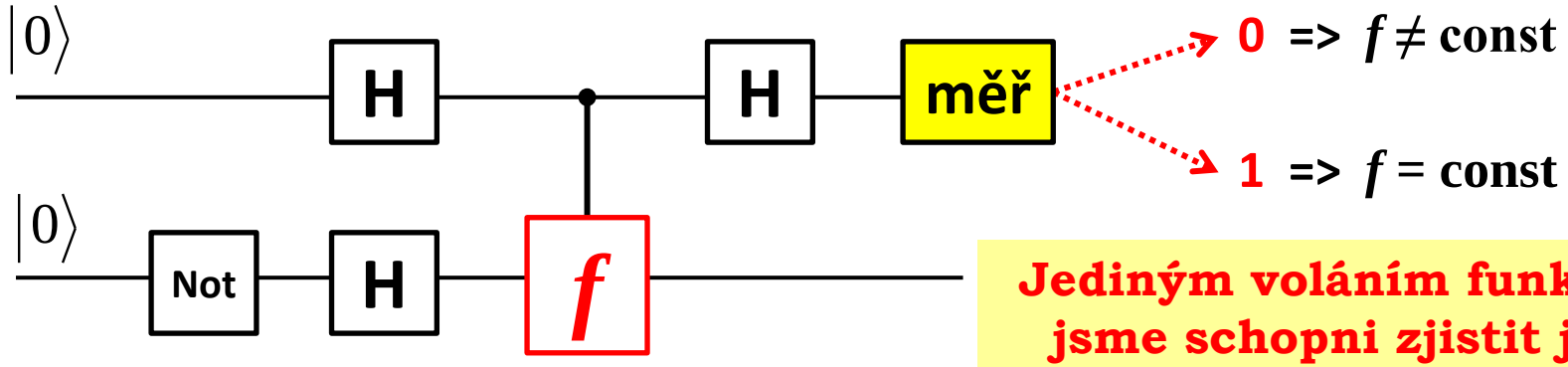


Vysvětlení:
Podle **Everettovy mnohosvětové interpretace** QM jsou jednotlivé členy kvantové superpozice „realizovány“ v různých „světech – vesmírech“. Paralelní vesmíry jsou ve vzájemném kontaktu po dobu udržení koherence kvantové superpozice. Vyšší efektivita kvantové počítání je důsledkem paralelismu výpočtů probíhajících v takových provázaných vesmírech …

Kvantové počítání

1) Historie
2) Principy
3) **Příklady**
4) Realizace

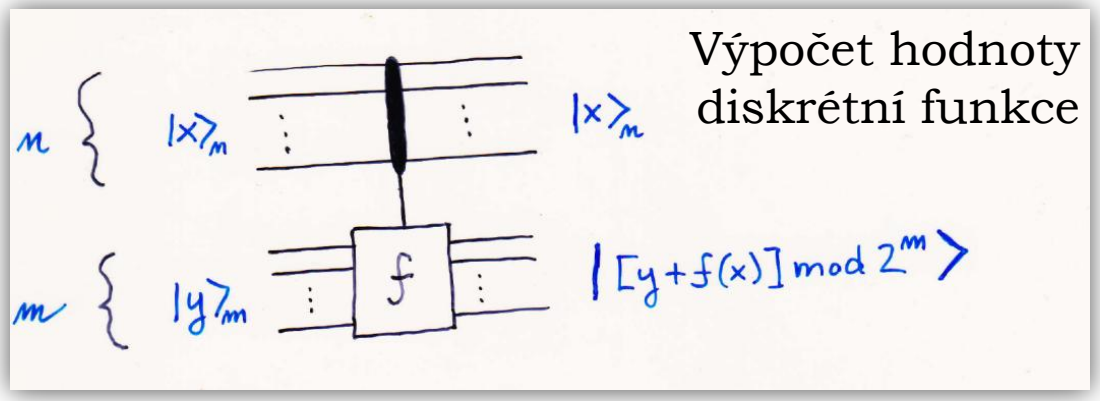
Testování funkcí například. test konstantnosti



Jediným voláním funkce jsme schopni zjistit její globální vlastnost !

2-bitová funkce

$x =$	$f(x) =$			
0	0	1	0	1
1	1	0	0	1
	≠ const		= const	

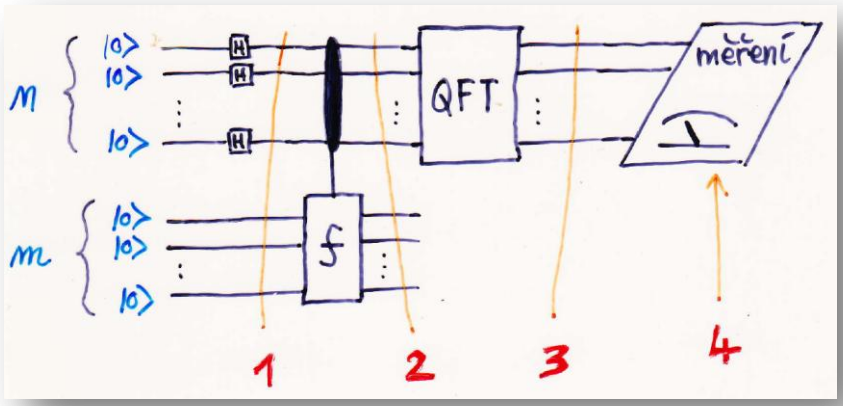


$$|x\rangle_n|0\rangle_m \rightarrow |x\rangle_n|f(x)\rangle_m$$

$$\sum_x \alpha_x |x\rangle_n|0\rangle_m \rightarrow \sum_x \alpha_x |x\rangle_n|f(x)\rangle_m$$

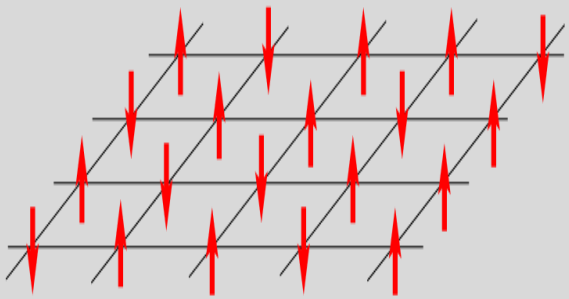
Další algoritmy

- **Prohledávání databází**
- **Shorův faktorizační algoritmus**
- Úlohy optimalizace ?
  Rozpoznávání obrazců ??
  Umělá inteligence ???
- **Simulace fyzikálních a chemických (biologických) systémů**



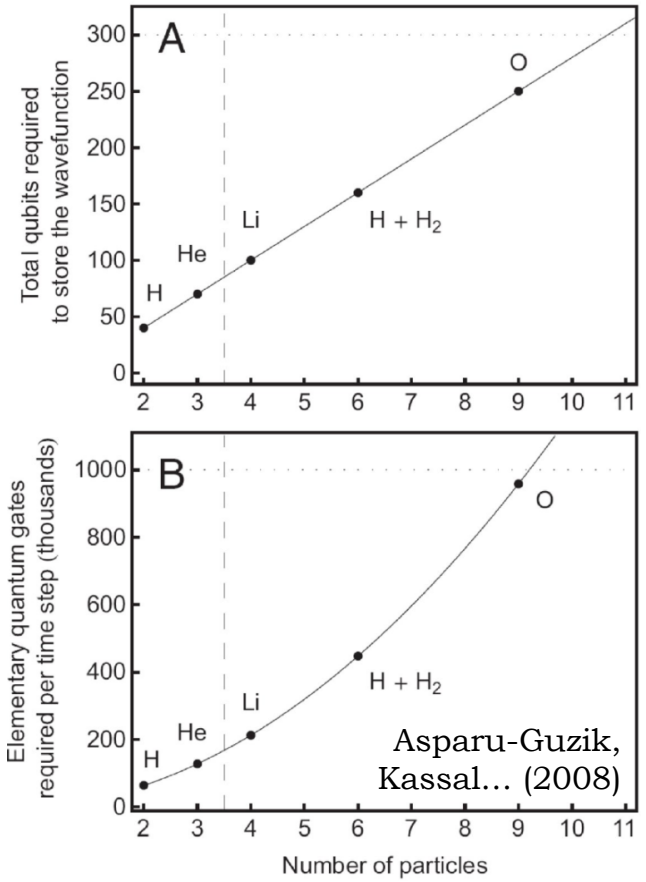
Mnohočásticový problém (jaderná fyzika, chemie…)

Počet bázových stavů systému (dimenze stavového prostoru) roste exponenciálně s počtem částic.
Např. 2D spinová mřížka: dimenze prostoru = 2^N



$N = 2\times 2 \Rightarrow \dim = 16$
$N = 3\times 3 \Rightarrow \dim = 512$
$N = 4\times 4 \Rightarrow \dim = 65.536$
$N = 5\times 5 \Rightarrow \dim = 33.554.432$
$N = 6\times 6 \Rightarrow \dim = 68.719.476.736$
$N = 7\times 7 \Rightarrow \dim = 562.949.953.421.312$
⋮

Možné aplikace při navrhování nových materiálů, chemicky/biologicky aktivních molekul…



Adiabatické kvantové počítání

$t = 0$ $\qquad$ $t = T$

pomalá (adiabatická) změna parametrů

in

out

$|\rightarrow\rightarrow\cdots\rightarrow\rangle$

„jednoduše připravitelný“ (při $T \to 0$) stav spinového systému

Př.: Problém splnitelnosti

Najít hodnoty N bitů $x_i \in \{0,1\}$, $i = 1,2,\ldots N$

splňující m klauzulí typu:

$$x_i + x_j + x_k = 1$$

$$i, j, k \in \{1,2,\ldots N\}$$

Problémy splnitelnosti obecně patří do třídy nepolynomiálních (NP-úplných) problémů!

$|\uparrow\downarrow\cdots\uparrow\rangle$

stav splňující zadanou soustavu klauzulí ($\downarrow \equiv 0$, $\uparrow \equiv 1$)

Farhi, Goldstone, Gutmann, Lapa, Lundgren, Preda, Science 292, 472 (2001)
Aharonov, van Dam, Kempe, Landau, Lloyd, Regev, SIAM J.Comput. 37, 166 (2007)

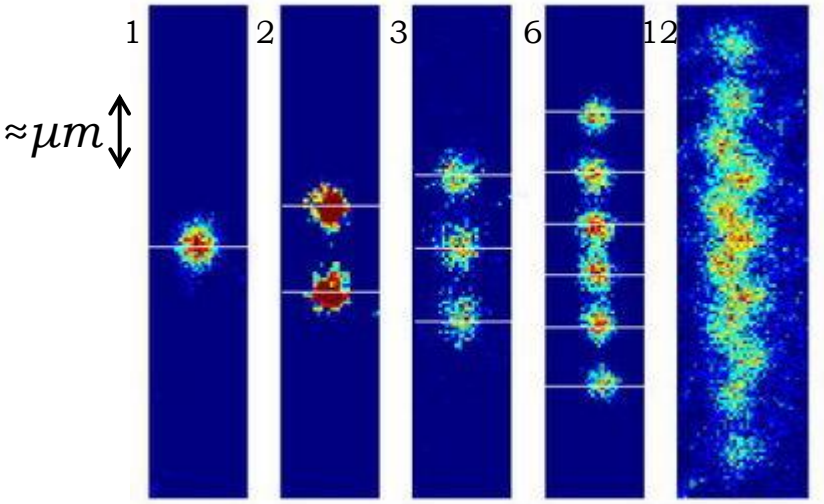
Kvantové počítání

1) Historie
2) Principy
3) Příklady
4) **Realizace**

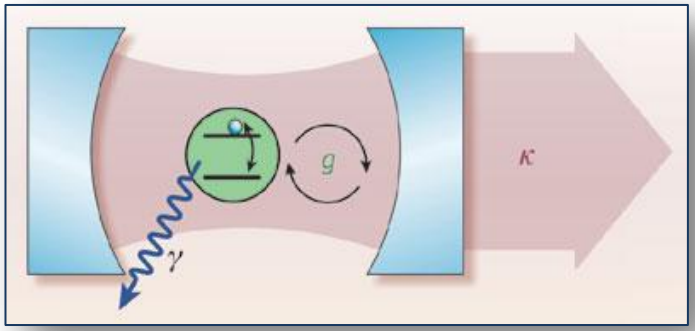
Technologie

a) Uvězněné ochlazené ionty
b) Kvantová elektrodynamika v dutině
c) Jaderná magnetická rezonance
d) Spinotronika v křemíku
e) Proudy v supravodivých smyčkách

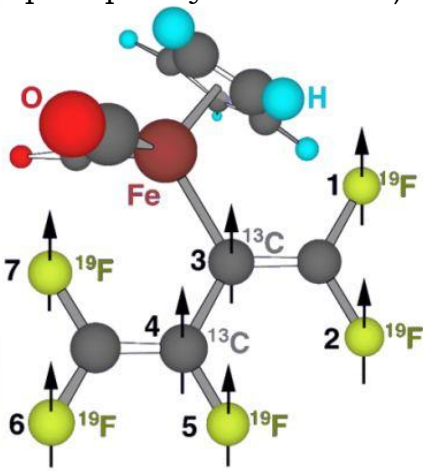
a) Uvězněné ionizované atomy (de)excitované laserem



b) Interakce atomů a záření v dutinovém rezonátoru



c) NMR v kapalné fázi (manipulace se spiny pomocí pulsů mag. pole s využitím spin-spinových interakcí)



Molekula se 7 Q-bity tvořenými jádry ^{13}C,^{19}F

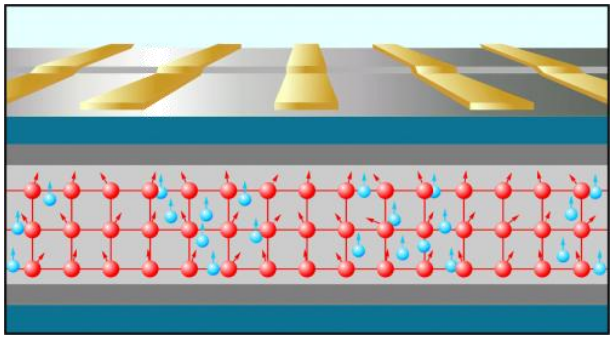
(pracuje se se statistickým souborem těchto jader)

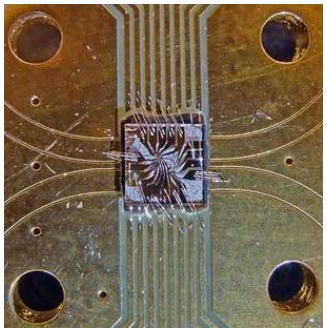
V roce 2001 proveden kvantový výpočet faktorizace

$$15 = 5 \times 3$$

V roce 2011 pomocí NMR implementace adiabatického kvantového výpočtu dosaženo: $143 = 13 \times 11$

d) Manipulace se spiny elektronů (jader) v polovodičové mříži

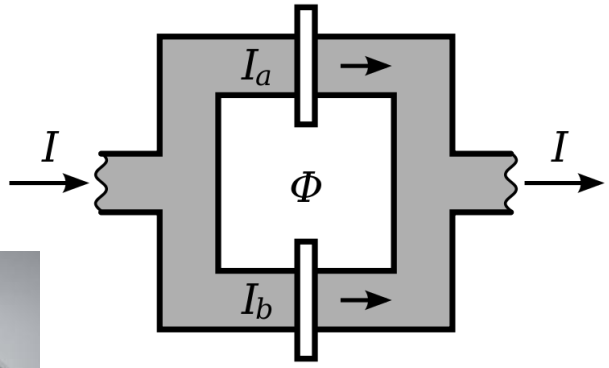


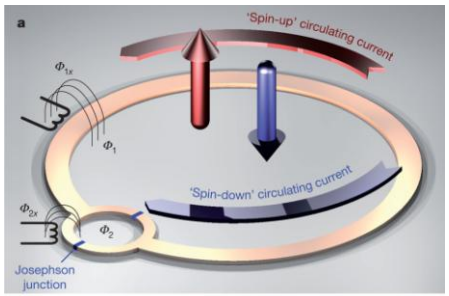


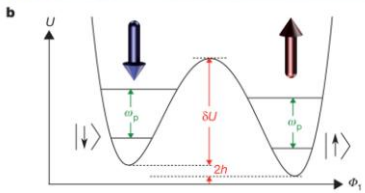
Technologie

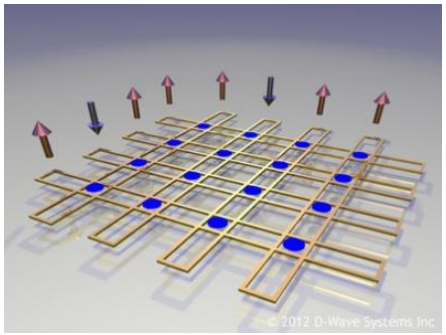
e) Makroskopické proudy v supravodivých smyčkách

SQUID:
Superconducting
Quantum
Interference
Device

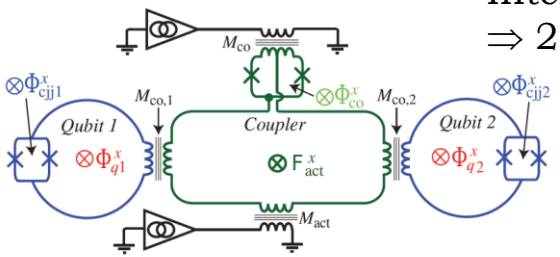








Interakce mezi SQUIDy
⇒ 2 qbitové operace



© D-Wave Systems

Johnson *et al.*, Nature 473, 194 (2011)

Překážky

DEKOHERENCE !!!

AUGUST 1996 PHYSICS TODAY

QUANTUM COMPUTING: DREAM OR NIGHTMARE?

Recent experiments have deepened our insight into the wonderfully counterintuitive quantum theory. But are they really harbingers of quantum computing? We doubt it.

Serge Haroche and Jean-Michel Raimond

ples of quantum
ıg were laid out
ars ago by com-
sts applying the
ɔn principle of
echanics to com-
tion. Quantum
ıas recently be-
topic in physics,
cognition that a
item can be pre-

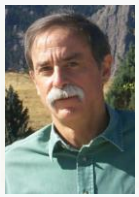
two interacting q
trol" bit and a
The control re
changed, but its
mines the evoluti
get: If the cc
nothing happens
if it is 1, the targ
a well-defined tra
Quantum m
mits additional

At this stage we think that some critical reflection is required in a field boiling with excitement. We feel that the enthusiasm is certainly justified, but not necessarily for the reasons generally adduced. Although the idea of quantum computing involves some fascinating new physics that goes far beyond the rather mundane problem of merely computing faster, we believe that performing large-scale calculations will remain an impossible dream for the foreseeable future.

Even if quantum computing remains a dream, the physics of quantum information processing at the level of a few qubits is fascinating. Experiments on entangled particles with ions in a trap or atoms in a cavity will help us understand the fundamental aspects of quantum measurement theory, and they may lead to major improvements in the precision spectroscopy of simple quantum systems.

Future of Quantum Computing Proves to Be Debatable

In presenting their opinions in the article "Quantum Computing: Dream or Nightmare?" (August, page 51), Serge Haroche and Jean-Michel Raimond conclude that large-scale quantum computation will remain merely a dream of computer theorists. Their principal argument is that, for a quantum computer to be useful, the ratio R of quantum gate speed to decoherence rate would have to be much higher than what can be obtained in the laboratory. Based on what has been achieved so far, this may be a safe bet. However, the subject is still in its infancy and at this time, its fundamental limits are not understood. Lacking such an understanding, Haroche and Raimond's pessimism about quantum computing is, in our opinion, premature.....

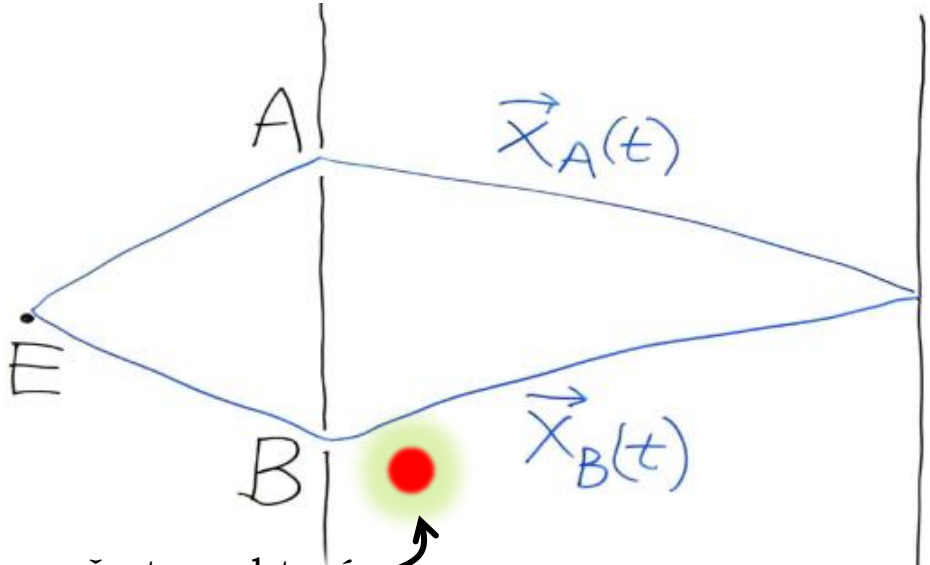


CHRISTOPHER MONROE
DAVID WINELAND
National Institute of Standards and Technology
Boulder, Colorado

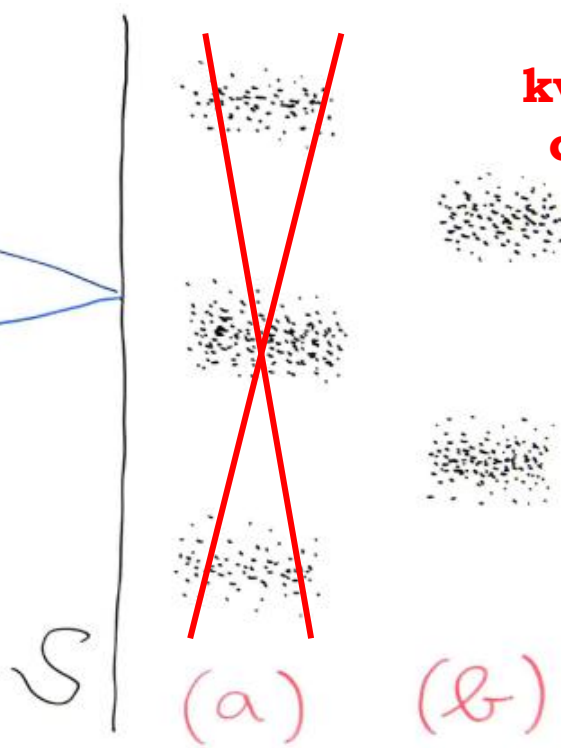
Překážky

DEKOHERENCE !!!

(a) koherentní superpozice		**(b) statistická směs**
$\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$	amplitudy ⟷ pravděpodobnosti	$p_0 = \|\alpha\|^2 \quad p_1 = \|\beta\|^2$
Pokud uskutečnění libovolné z alternativ *nelze* principiálně zjistit (např. měřením na jiném objektu) **=> interference**		Pokud uskutečnění některé z alternativ *lze* potenciálně zjistit (např. měřením na jiném objektu) **=>** ~~interference~~



Objekt, např.atom, který monitoruje dráhu elektronu uvnitř přístroje (z jeho kvantového stavu se dá jednoznačně zjistit, kterou ze štěrbin elektron prošel)



Konec kvantového chování !!!

Překážky

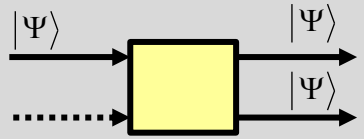
~~DEKOHERENCE~~ !!!

(a) koherentní superpozice		**(b) statistická směs**
$\|\psi\rangle = \alpha\|0\rangle + \beta\|1\rangle$	amplitudy ⟷ pravděpodobnosti	$p_0 = \|\alpha\|^2 \quad p_1 = \|\beta\|^2$
Pokud uskutečnění libovolné z alternativ *nelze* principiálně zjistit (např. měřením na jiném objektu) => **interference**		Pokud uskutečnění některé z alternativ *lze* potenciálně zjistit (např. měřením na jiném objektu) => ~~interference~~

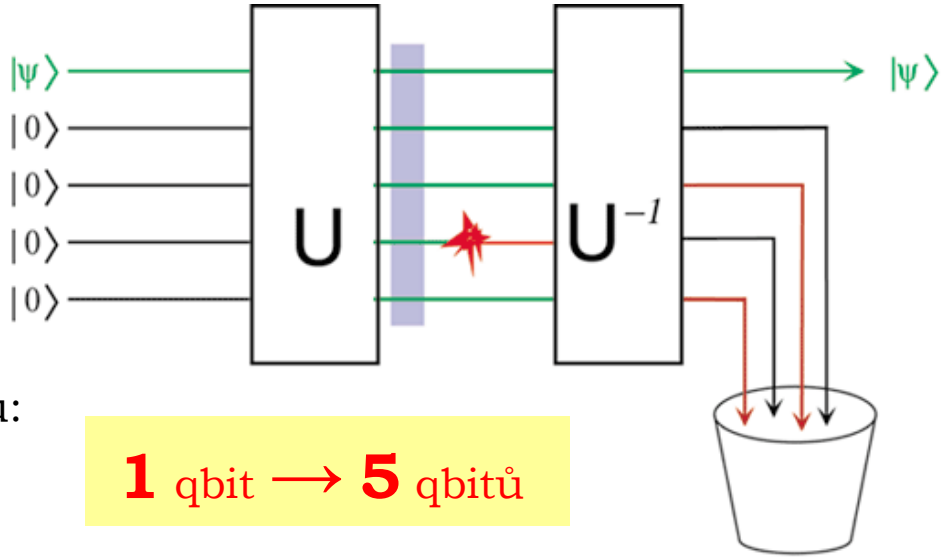
Opravné procedury využívající redundanci

Ne však prosté „namnožení“ qbitu – tomu brání **kvantový *“no-cloning”* teorém**:

Je v principu **nemožné** sestrojit zařízení, které by vytvářelo 2 nebo více replik obecného (neznámého) kvantového stavu (bylo by to v rozporu s vlastnostmi kvantové dynamiky).



Možnost opravy obecné chyby, pokud vznikla pouze na jednom (libovolném) qbitu:



1 qbit ⟶ **5** qbitů

MFF UK Praha, laboratoře Trója, rok 3046